

## § 2001.47

its representative a signed receipt is required.

(f) *Receipt of classified information.* Agency heads shall establish procedures which ensure that classified information is received in a manner which precludes unauthorized access, provides for inspection of all classified information received for evidence of tampering and confirmation of contents, and ensures timely acknowledgment of the receipt of Top Secret and Secret information by an authorized recipient. As noted in paragraph (e) of this section, a receipt acknowledgment of all classified material transmitted to a foreign government or its representative is required.

## § 2001.47 Destruction.

Classified information identified for destruction shall be destroyed completely to preclude recognition or reconstruction of the classified information in accordance with procedures and methods prescribed by agency heads. The methods and equipment used to routinely destroy classified information include burning, cross-cut shredding, wet-pulping, melting, mutilation, chemical decomposition or pulverizing. Agencies shall comply with the destruction equipment standard stated in § 2001.42(b) of this Directive.

## § 2001.48 Loss, possible compromise or unauthorized disclosure.

(a) *General.* Any person who has knowledge that classified information has been or may have been lost, possibly compromised or disclosed to an unauthorized person(s) shall immediately report the circumstances to an official designated for this purpose.

(b) *Cases involving information originated by a foreign government or another U.S. government agency.* Whenever a loss or possible unauthorized disclosure involves the classified information or interests of a foreign government agency, or another U.S. government agency, the department or agency in which the compromise occurred shall advise the other government agency or foreign government of the circumstances and findings that affect their information or interests. However, foreign governments normally will not be advised

## 32 CFR Ch. XX (7–1–13 Edition)

of any security system vulnerabilities that contributed to the compromise.

(c) *Inquiry/investigation and corrective actions.* Agency heads shall establish appropriate procedures to conduct an inquiry/investigation of a loss, possible compromise or unauthorized disclosure of classified information, in order to implement appropriate corrective actions, which may include disciplinary sanctions, and to ascertain the degree of damage to national security.

(d) *Reports to ISOO.* In accordance with section 5.5(e)(2) of the Order, agency heads or senior agency officials shall notify the Director of ISOO when a violation occurs under paragraphs 5.5(b)(1), (2), or (3) of the Order that:

(1) Is reported to oversight committees in the Legislative branch;

(2) May attract significant public attention;

(3) Involves large amounts of classified information; or

(4) Reveals a potential systemic weakness in classification, safeguarding, or declassification policy or practices.

(e) *Department of Justice and legal counsel coordination.* Agency heads shall establish procedures to ensure coordination with legal counsel whenever a formal action, beyond a reprimand, is contemplated against any person believed responsible for the unauthorized disclosure of classified information. Whenever a criminal violation appears to have occurred and a criminal prosecution is contemplated, agency heads shall use established procedures to ensure coordination with:

(1) The Department of Justice, and

(2) The legal counsel of the agency where the individual responsible is assigned or employed.

## § 2001.49 Special access programs.

(a) *General.* The safeguarding requirements of this Directive may be enhanced for information in special access programs (SAP), established under the provisions of section 4.3 of the Order by the agency head responsible for creating the SAP. Agency heads shall ensure that the enhanced controls are based on an assessment of the value, critical nature, and vulnerability of the information.

(b) *Significant interagency support requirements.* Agency heads must ensure that a Memorandum of Agreement/Understanding is established for each SAP that has significant interagency support requirements, to appropriately and fully address support requirements and supporting agency oversight responsibilities for that SAP.

**§ 2001.50 Telecommunications automated information systems and network security.**

Each agency head shall ensure that classified information electronically accessed, processed, stored or transmitted is protected in accordance with applicable national policy issuances identified in the Committee on National Security Systems (CNSS) issuances and the Intelligence Community Directive (ICD) 503, *Intelligence Community Information Technology Systems Security Risk Management, Certification, and Accreditation*.

**§ 2001.51 Technical security.**

Based upon the risk management factors referenced in § 2001.40 of this directive, agency heads shall determine the requirement for technical countermeasures such as Technical Surveillance Countermeasures and TEMPEST necessary to detect or deter exploitation of classified information through technical collection methods and may apply countermeasures in accordance with NSTISSI 7000, *TEMPEST Countermeasures for Facilities*, and SPB Issuance 6-97, *National Policy on Technical Surveillance Countermeasures*.

**§ 2001.52 Emergency authority.**

(a) Agency heads or any designee may prescribe special provisions for the dissemination, transmission, safeguarding, and destruction of classified information during certain emergency situations.

(b) In emergency situations, in which there is an imminent threat to life or in defense of the homeland, agency heads or designees may authorize the disclosure of classified information to an individual or individuals who are otherwise not routinely eligible for access under the following conditions:

(1) Limit the amount of classified information disclosed to the absolute minimum to achieve the purpose;

(2) Limit the number of individuals who receive it;

(3) Transmit the classified information via approved Federal Government channels by the most secure and expeditious method to include those required in § 2001.46, or other means deemed necessary when time is of the essence;

(4) Provide instructions about what specific information is classified and how it should be safeguarded; physical custody of classified information must remain with an authorized Federal Government entity, in all but the most extraordinary circumstances;

(5) Provide appropriate briefings to the recipients on their responsibilities not to disclose the information and obtain a signed nondisclosure agreement;

(6) Within 72 hours of the disclosure of classified information, or the earliest opportunity that the emergency permits, but no later than 30 days after the release, the disclosing authority must notify the originating agency of the information by providing the following information:

(i) A description of the disclosed information;

(ii) To whom the information was disclosed;

(iii) How the information was disclosed and transmitted;

(iv) Reason for the emergency release;

(v) How the information is being safeguarded; and

(vi) A description of the briefings provided and a copy of the nondisclosure agreements signed.

(7) Information disclosed in emergency situations shall not be required to be declassified as a result of such disclosure or subsequent use by a recipient.

**§ 2001.53 Open storage areas.**

This section describes the minimum construction standards for open storage areas.

(a) *Construction.* The perimeter walls, floors, and ceiling will be permanently constructed and attached to each other. All construction must be done in